Case 1:
Due to the fact that the protection measures for student account information at a certain university are only ``Recommendation'' and lack mandatory and punitive mechanisms, students' awareness of personal information security is weak. A social engineer exploited this loophole and carried out social engineering attacks of impersonation and intimidation. The attacker pretended to be a staff member of the Academic Affairs Office of the University and contacted the students through a forged official telephone number, claiming that the purpose of checking the information was to ensure that the scholarship was granted correctly, thus defrauding the students' personal information such as name, student number, ID number, etc. Subsequently, the attackers further threatened the students on the grounds that ``abnormal credits'' may affect their academic status and demanded that they pay a ``student status protection fund'' to avoid suspension. Under pressure, the victimized student provided personal information and transferred payment, only to eventually discover that he had been deceived into taking money.

Case 2:
A certain IT company requires employees to update their work permissions every quarter to ensure system security, but due to the lack of mandatory reminders, employees have overlooked information protection. A social engineer utilized this modal constraints defect to carry out attacks through shoulder surfing and incentive manipulation. In the coffee shop where employees often go, attackers obtain the identification information of an IT employee by shoulder surfing. Subsequently, the attacker used forged internal emails to contact the employee under the pretext of high-performance rewards, falsely claiming that they needed to evaluate the progress of internal projects to determine reward allocation, and further deceived them into revealing sensitive information such as the upcoming software release date. In the end, the attacker not only successfully entered the company's network but also obtained the company's core secrets, resulting in the new software release plan being preempted by competitors and causing serious losses to the company.

Case 3:
Company A is a large advertising company, and its advertising department manager is responsible for confirming cooperation projects. However, due to the lack of clear regulations on the specific form or notification method for confirming cooperation intentions, there is a deficiency in modal constraints. A social engineer exploited this vulnerability to launch attacks through tailgating, distraction, and incentive manipulation. The attacker followed the advertising department manager into the company and then chatted with him in the elevator, distracting his attention, gaining his trust, and obtaining

personal information such as name and position. Subsequently, the attacker induced the advertising department manager to discuss and leak details of the collaboration and gift plan information by mentioning a special advertising cooperation plan and its "promotional gifts." Due to the lack of strict verification mechanisms and standards in the company, the manager was unable to identify the threat, and the attacker successfully obtained sensitive information.

Case 4:
A social engineering attack occurred in the academic administration system of a certain university due to the lack of clear information verification and security verification processes due to modal constraint defects. The attacker searched through dumpster diving to obtain information such as the name, contact information, and work arrangements of the academic affairs teacher. They used this information to impersonate themselves as leaders of the academic affairs office and successfully deceived the IT department into resetting the academic affairs teacher's account password. Subsequently, the attacker sent forged task emails, using a responsibility manipulation strategy to pressure academic teachers to provide student grades and test paper information, claiming that any delay would affect student graduation evaluations. The victim sent sensitive information without verifying their identity in a tense situation due to a lack of verification mechanisms and prevention awareness. The attacker ultimately obtains students' grades, test papers, and other private data, which will lead to issues such as identity theft and fraud.